CLAIMS

What is claimed is:

1. A method for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, whereby each of the subscriber nodes and the publisher nodes receives a unique private key and that can determine events that the subscribers and the publishers may process, the method comprising the steps of:

registering the subscribers and the publishers with an event server configured to determine whether the publishers are authorized to produce certain events corresponding to the event types and whether the subscribers are authorized to receive the certain events in response to the step of accessing;

generating, with the event server, a group session key for establishing one of the multicast groups, the group session key being encrypted in a message that has a prescribed format.

2. The method as recited in Claim 1, further comprising the steps of:

receiving a message from the subscribers in response to the subscribers determining whether the received message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

sub 3.99 The method as recited in Claim 1, wherein the prescribed format of the message conforms with lightweight directory access protocol (LDAP).

4. The method as recited in Claim 1, wherein the prescribed format of the message comprises a protocol version number field, a message type field, and a message length field.

5. The method as recited in Claim 1, wherein the step of authenticating comprises controlling access by the directory in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

6. The method as recited in Claim 1, wherein the external authentication service is ~~supplied by a Kerberos server.~~

7. The method as recited in Claim 1, wherein the event server manages the private keys of the subscribers and the publishers.

sub 8.05 The method as recited in Claim 1, wherein the step of updating comprises:
creating a new group session key;
modifying the objects based upon the new group session key by using a change password protocol;
sending a new message that contains the new group session key to the subscribers; and
notifying the subscribers to reregister.

9. The method as recited in Claim 1, wherein the step of registering comprises performing access control check of the subscribers by the event server.

sub AC

10. A communication system for creating a plurality of secure multicast groups in a network that includes a plurality of principals configured for functioning as a subscriber and a publisher, each of the principals having a private key, a multi-master directory comprising a directory server for communicating with one or more of the principals to authenticate each of the principals and to provide access control, the multi-master directory controlling access on a per object and per attribute basis, the communication system comprising:

an event server coupled to the plurality of principals for registering the plurality of principals and for determining whether the principals are authorized to produce certain events when the principals are functioning as publishers and whether the principals are authorized to receive the certain events when the principals are functioning as subscribers; and

means in the event server for creating a group session key for establishing one of the multicast groups, by distributing the group session key in an encrypted message to the subscribers, the encrypted message encapsulating the group session key according to a prescribed format;

means in the event server for updating the group session key by utilizing a change password protocol to modify an object in the directory;

means in the event server for notifying the subscribers to reregister in response to the updating of the group session key.

11. The communication system as recited in Claim 10, wherein the directory server is collocated with the event server, the directory server and the event server participating in a common one of the multicast groups.

12. The communication system as recited in Claim 10, wherein the prescribed format of the message conforms with lightweight directory access protocol (LDAP).

13. The communication system as recited in Claim 10, wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

14. The communication system as recited in Claim 13, wherein the external authentication service is supplied by a Kerberos server.

15. The communication system as recited in Claim 10, wherein the prescribed format of the message comprises a protocol version number field, a message type field, and a message length field.

16. The communication system as recited in Claim 10, wherein the event server manages the private keys.

17. The communication system as recited in Claim 10, wherein the event server updates the group session key by performing the steps of:
creating a new group session key;

modifying the objects based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

18. The communication system as recited in Claim 10, wherein the event server performs access control check of the subscribers during registration of the subscribers.

Sub 19. A computer system for establishing multiple secure multicast groups, the computer system comprising:

a communication interface for communicating with a plurality of nodes and for interfacing a multi-master directory to authenticate the computer system and the plurality of nodes, the multi-master directory having access controls on a per object and per attribute basis, wherein the nodes access the directory to determine events that the nodes may process;

a bus coupled to the communication interface for transferring data;

one or more processors coupled to the bus for selectively generating a group session key and private keys corresponding to the plurality of nodes, the group session key being updated by utilizing a change password protocol to modify an object corresponding to the events in the directory; and

a memory coupled to the one or more processors via the bus, the memory including one or more sequences of instructions which when executed by the one or more processors cause the one or more processors to perform the steps of registering the plurality of nodes, determining whether the nodes are authorized to produce and authorized to receive certain events

corresponding to objects of the directory, distributing the group session key to the nodes via a message, the message encapsulating the group session key according to a prescribed format, and selectively reregistering the nodes in response to updating the group session key.

20. The computer system as recited in Claim 19, wherein the directory server is collocated with the event server, the directory server and the event server participating in a common one of the multicast groups.

21. The computer system as recited in Claim 19, wherein the prescribed format of the message conforms with light weight directory access protocol (LDAP).

22. The computer system as recited in Claim 19, wherein the directory authenticates by using authentication services of the directory in conjunction with a Kerberos service that allows extending membership to the multicast groups to nodes with no objects in the directory.

23. The computer system as recited in Claim 19, wherein the event server manages private keys of the plurality of nodes.

24. The computer system as recited in Claim 19, wherein the event server updates the group session key by performing the steps of:

creating a new group session key;

modifying the objects based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

25. The computer system as recited in Claim 19, wherein the computer system performs access control check of the nodes during registration.

26. A computer-readable medium carrying one or more sequences of instructions for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, whereby each of the subscriber nodes and the publisher nodes receives a unique private key and that can determine events that the subscribers and the publishers may process, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering the subscribers and the publishers with an event server, the event server determining whether the publishers are authorized to produce certain events corresponding to the event types and whether the subscribers are authorized to receive the certain events in response to the step of accessing;

generating a group session key for establishing one of the multicast groups, the group session key being encrypted in a message that has a prescribed format.

27. A computer-readable medium as recited in Claim 26, further comprising the steps of:

receiving a message from the subscribers in response to the subscribers determining whether the received message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

28. A computer-readable medium as recited in Claim 26, wherein the step of authenticating comprises controlling access by the directory in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

29. A computer-readable medium as recited in Claim 26, wherein the step of updating comprises:

creating a new group session key;

modifying the objects based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

30. A computer-readable medium as recited in Claim 26, wherein the step of registering comprises performing access control check of the subscribers by the event server.